RATIONAL CURVES AND POINTS ON K3 SURFACES

by

Fedor Bogomolov and Yuri Tschinkel

Abstract. — We study the distribution of algebraic points on K3 surfaces.

Contents

1. Introduction

Let k be a field and $\bar{k}$ a fixed algebraic closure of k. We are interested in connections between geometric properties of algebraic varieties and their arithmetic properties over k, over its finite extensions k'/k or over $\bar{k}$. Here we study certain varieties of intermediate type, namely K3 surfaces and their higher dimensional generalizations, Calabi-Yau varieties.

To motivate the following discussion, consider a K3 surface S defined over k. In positive characteristic, S may be unirational and covered by rational curves. If k has characteristic zero, then S contains countably

many rational curves, at most finitely many in each homology class of S (the counting of which is an interesting problem in enumerative geometry, see [**4**], [**6**], [**8**], [**24**]). Over uncountable fields, there may, of course, exist k-rational points on S not contained in any rational curve defined over $\bar{k}$. The following extremal statement, proposed by the first author in 1981, is however still a logical possibility:

Let k be either a finite field or a number field. Let S be a K3 surface defined over k. Then every $\bar{k}$-rational point on S lies on some rational curve $C \subset S$, defined over $\bar{k}$.

In this note we collect several representative examples illustrating this statement. One of our results is:

Theorem 1.1. — *Let S be a Kummer surface over a finite field k. Then every $s \in S(\bar{k})$ lies on a rational curve $C \subset S$, defined over $\bar{k}$.*

Using this theorem we produce examples of non-uniruled but "rationally connected" surfaces over finite fields (any two algebraic points can be joined by a chain of rational curves).

Acknowledgments: We are grateful to Brendan Hassett, Ching-Li Chai, Nick Katz, Barry Mazur and Bjorn Poonen for their interest and comments.

2. Preliminaries: abelian varieties

In this section we collect some facts concerning abelian varieties. Our basic reference is [**14**].

Let A be an abelian variety over $\bar{k}$, $A[n] \subset A(\bar{k})$ the set of the n-torsion points of A. If k is finite, then every point in $A(\bar{k})$ is a torsion point. For every torsion point $x \in A(\bar{k})$ let

$$\mathrm{ord}(x) := \min\{n \in \mathbb{N} \mid nx = 1\}$$

be the order of x. An elliptic curve E over a field k of characteristic p is called *supersingular* if its p-rank is zero, an abelian variety over k

is called supersingular if it is $\bar{k}$-isogenous to a product of supersingular elliptic curves.

Recall that every abelian variety A, defined over $\bar{k}$, is isogenous to a product of *simple* abelian varieties (over $\bar{k}$). The ring $\mathrm{End}_{\bar{k}}(A)$ of $\bar{k}$-endomorphisms of a simple abelian variety A is a maximal order in some finite dimensional division algebra D over $\mathbb{Q}$, of dimension d^2 over its center Z_D. Here Z_D is a finite extension of $\mathbb{Q}$ of degree e. If k is finite, then $ed = 2\dim(A)$, that is, A has complex multiplication.

Remark 2.1. — In our applications, we will use hyperelliptic curves contained in abelian varieties. Recall that, over an algebraically closed field, every abelian surface is the Jacobian of a (possibly reducible) hyperelliptic curve (see [**23**]). A simple argument shows that for any abelian variety A over $\mathbb{C}$ (in any dimension) the set of hyperelliptic curves which have a Weierstrass point (fixed point of the hyperelliptic involution) at the origin of A is at most discrete. Indeed, a family of such curves would give a uniruled surface in the quotient A/σ (under the standard multiplication by -1 map σ). However, A/σ has nontrivial holomorphic two-forms which extend to its desingularization. They cannot restrict to a uniruled surface. A much more precise result is proved in [**16**]: a generic principally polarized abelian variety of dimension ≥ 3 over $\mathbb{C}$ does not contain *any* hyperelliptic curves. Similarly, a generic abelian variety of dimension ≥ 4 does not contain trigonal curves [**1**]. A similar result holds in positive characteristic, over *large* fields, like an algebraic closure of $\bar{\mathbb{F}}_q(t)$ [**15**].

It could still be possible that over an algebraic closure of a *finite* field, every abelian variety contains a hyperelliptic curve.

Let C be a smooth projective geometrically connected curve of genus $\mathsf{g} = \mathsf{g}(C)$ over a field k and $J = J_C$ the Jacobian of C. Throughout, we assume that $C(k) \neq \emptyset$ and choose a point $c_0 \in C(k)$ which we use to identify the degree n Jacobian $J_C^{(n)}$ with J_C and to embed $C \to J_C$. Consider the maps

$$
\begin{array}{ccccccc}
C^n & \longrightarrow & C \times \mathrm{Sym}^{(n-1)}(C) & \xrightarrow{\phi_n} & \mathrm{Sym}^{(n)}(C) & \xrightarrow{\varphi_n} & J_C^{(n)} \\
 & & & & & & \\
c = (c_1, \dots, c_n) & \longrightarrow & (c_1, c_2 + \cdots + c_n) & \longrightarrow & (c_1 + \cdots + c_n) & \longrightarrow & [c]
\end{array}
$$

The map ϕ_n is a (finite, non-Galois for $n \geq 3$) cover of degree n. For all $n \geq 2\mathsf{g}+1$, the map φ_n is a $\mathbb{P}^{n-\mathsf{g}}$-bundle and the map $C^n \to J^{(n)}(C)$ has geometrically irreducible fibers (see [**12**], Cor. 9.1.4, for example).

Lemma 2.2. — *Let k be a number field or a (sufficiently large) finite field with a fixed algebraic closure $\bar{k}$. Let C be a smooth projective geometrically connected curve over k of genus $\mathsf{g} = \mathsf{g}(C) \geq 1$, with Jacobian $J = J_C$. For every $n \geq 2\mathsf{g}+1$ and every point $x \in J(k)$ there exists a point $y \in \varphi_n^{-1}(x)$, defined over k, whose preimage $c = (c_1, \dots, c_n) \in C^n(\bar{k})$ gives rise to a k-irreducible degree n zero-cycle $c_1 + \cdots + c_n$ on C.*

Proof. — Let $x \in J(k)$ be a point and $\mathbb{P}_x = \varphi_n^{-1}(x) \subset \mathrm{Sym}^{(n)}(C)$ the fiber over x. The restriction $\phi_{n,x}$ of ϕ_n to $\mathbb{P}_x$ is a (nontrivial) cover of degree n. Using Chebotarev density (or an equidistribution theorem, as in [**12**], Th. 9.4.4) we find that, if k is sufficiently large (either a number field, or a finite field with $\geq \mathsf{c}(\mathsf{g})$ elements, where $\mathsf{c}(\mathsf{g})$ is an explicit constant depending only on the genus g), there exists a point $y \in \mathbb{P}_x$ such that the fiber $\phi_{n,x}^{-1}(y)$ is irreducible over k. □

Remark 2.3. — The same statement holds for quasi-projective curves C and their (generalized) Jacobians.

A similar result (over finite fields) has recently been used in [**17**], Lemma 5.

We reformulate the above theorem in a more convenient form:

Corollary 2.4. — *Let C be a curve of genus $\mathsf{g} = \mathsf{g}(C) \geq 2$ over a number field K and $J = J_C$ its Jacobian. Assume that C has a zero-cycle of degree $n = 2\mathsf{g}+1$ over K and use this cycle to identify $J^{(n)} = J$ and the embedding $C \to J$. For any point $x \in J(K)$ there exists an extension K'/K of degree n and a point $c \in C(K')$ such that the cycle $\mathrm{Tr}_{K'/K}(c) = x \in J^{(n)}(K) = J(K)$.*

Corollary 2.5. — *Let C be a curve of genus $\mathsf{g}(C) \geq 2$ over a (sufficiently large) finite field k, $J = J_C$ its Jacobian and $x \in J(k)$ a point. Choose a point c_0 on $C(k)$ and use it to identify $J_C = J_C^{(n)}$, for all n, and to embed $C \to J_C$. Then there exist a point $c \in C(\bar{k})$ and infinitely many endomorphisms $\Phi \in \mathrm{End}_{\bar{k}}(J)$ such that $\Phi(c) = x$.*

Proof. — For any $n \geq 2\mathsf{g}(C) + 1$ consider the surjective map φ_n. Let $x \in J_C^{(n)}(k)$ be a point and $\mathbb{P}_x = \varphi_n^{-1}(x)$ the projective space over x, parametrizing all zero-cycles equivalent to x. Extending k, if necessary, we find a $y \in \mathbb{P}_x(k)$ such that the fiber

$$\phi_n^{-1}(y) = \{(c_1, c_2 + \cdots + c_n), (c_2, c_1 + \cdots + c_n), \ldots, (c_n, c_1 + \cdots + c_{n-1})\}$$

is irreducible over k (see [**12**], Th. 9.4.4).

We can write $y = \sum_{g \in G} c^g$, with $c := c_1 \in C(k')$, where k'/k is the (unique) extension of k of degree n and g runs through the (cyclic) Galois group $G := \mathrm{Gal}(k'/k)$ over k. Note that g are simply (distinct) powers of the Frobenius morphism. We have

$$y = \sum_{j=0}^{n-1} \mathrm{Fr}^j(c).$$

Now note that the Frobenius morphism "lifts" to a k'-endomorphism of J, that is, the Frobenius endomorphism $\tilde{\mathrm{Fr}} \in \mathrm{End}_{\bar{k}}(J)$ acts on $J(k')$ in the same way as the Galois automorphism $\mathrm{Fr} \in \mathrm{Gal}(k'/k)$. Put

$$\Phi := \sum_{j=0}^{n-1} \tilde{\mathrm{Fr}}^j,$$

as an element of $\mathrm{End}_{\bar{k}}(J)$. Changing n, we get infinitely many such endomorphisms (over $\bar{k}$). □

Remark 2.6. — In particular, Corollary 2.5 implies that if $\mathrm{ord}(x) = m$ then, for any embedding of $C \subset J_C$, there exist infinitely many points in $C(\bar{k}) \subset J_C(\bar{k})$ whose order is divisible by m. Indeed, notice that $\mathrm{ord}(c) = \mathrm{ord}(c^g)$, for all $g \in \mathrm{Gal}(k'/k)$, (with respect to some group law on the set $J(k)$). Since the order of x (and y) is m the order $\mathrm{ord}(c)$ is divisible by m.

A related result has been proved in [**2**]: Let ℓ be a prime, C a curve, $J = J_C$ its Jacobian (defined over a finite field k), $C \subset J$ a *fixed* embedding

and $\lambda : J(\bar{k}) \to J(\bar{k})_\ell$ the projection onto the ℓ-primary part. Then the map $\lambda : C(\bar{k}) \to J(\bar{k})_\ell$ is surjective. It was noticed in [**18**] that this fact implies that any positive-dimensional subvariety of a geometrically simple abelian variety (over a finite field) contains infinitely many points of pairwise prime orders.

The same argument gives a statement very much in the spirit of [**11**]:

Corollary 2.7. — *Let C be a curve of genus g over a sufficiently large finite field k, $J = J_C$ its Jacobian and k'/k the (unique) degree $2\mathsf{g}+1$ extension of k. Then there exists a morphism $C \to J$ (depending on k) such that $J(k) \subset C(k')$.*

3. Preliminaries: K3 surfaces

We assume that the characteristic of k is either zero or at least 7.

Definition 3.1. — *A connected simply-connected projective algebraic surface with trivial canonical class is called a K3 surface. A K3 surface S with* $\operatorname{rk}\operatorname{Pic}(S) = 22$ *is called* supersingular.

Example 3.2. — Typical K3 surfaces are double covers of $\mathbb{P}^2$ ramified in a smooth curve of degree 6, smooth quartic hypersurfaces in $\mathbb{P}^3$ or smooth intersections of 3 quadrics in $\mathbb{P}^5$.

Another interesting series of examples is given by (generalized) Kummer surfaces: desingularizations of quotients of abelian surfaces by certain finite group actions (see Proposition 4.4).

Remark 3.3. — If S is a K3 surface over a field of characteristic zero, then $\operatorname{rk}\operatorname{Pic}(S) \leq 20$. An example of a supersingular S over a field of positive characteristic is given by a desingularization of A/σ, where A is a supersingular abelian variety and σ the standard involution (multiplication by -1 map).

Remark 3.4. — If $\operatorname{rk}\operatorname{Pic}(S) < 22$ (and hence ≤ 20) then the Brauer group of S has nontrivial transcendental part. In particular, S is not uniruled. This is always the case in characteristic zero. Over fields of positive characteristic, there may exist uniruled K3 surfaces, with necessarily the maximal possible Picard number $\operatorname{rk}\operatorname{Pic}(S) = 22$ (all cycles are algebraic); and they are therefore supersingular [**20**], [**3**].

In characteristic 2, every supersingular K3 surface is unirational [**19**]. It is conjectured that all supersingular K3 surfaces are unirational. A generalized Kummer surface $S \sim A/G$ is uniruled iff it is unirational iff the corresponding abelian surface A is supersingular [**21**], [**10**].

4. Construction

We recall the classical construction of special K3 surfaces, called *Kummer* surfaces. Let A be an abelian surface,

$$\begin{array}{rccc} \sigma\,:\, A & \to & A \\ a & \mapsto & -a \end{array}$$

the standard involution. The set of fixed points of σ is exactly $A[2]$. The blowup $S := \widehat{A/\sigma}$ of the image of $A[2]$ in the quotient A/σ is a smooth K3 surface S, called a *Kummer* surface:

$$\pi\,:\, A/\sigma \to S, \qquad \hat{\pi}\,:\, \widehat{A/\sigma} \to S.$$

Consider rational curves in A/σ.

Lemma 4.1. — *Rational curves $C \in A/\sigma$ correspond to hyperelliptic curves $\tilde{C} \subset A$ containing a two-torsion point $P \in A[2]$.*

Proof. — The hyperelliptic involution on C acts as an involution σ : $x \to -x$ on the Jacobian J_C and hence also on the abelian subvariety which is the image of J_C in A. In particular, the involution σ on A induces the standard hyperelliptic involution on C. Hence $C/\sigma = \mathbb{P}^1$ is rational and defines a rational curve in A/σ. Conversely, if $\mathbb{P}^1 \in A/\sigma$ is rational then the preimage of $\mathbb{P}^1$ in A is irreducible (since A doesn't contain rational curves). Thus $\mathbb{P}^1 = \tilde{C}/\sigma$ and $\tilde{C}$ is hyperelliptic and all ramification points of the map $\tilde{C} \to C = \mathbb{P}^1$ are contained among the two-torsion points $A[2] \cap \tilde{C}$. □

Theorem 4.2. — *Let k be a finite field, C a curve of genus 2 defined over k, $J = J_C$ its Jacobian surface and $S \sim J/\sigma$ the associated Kummer surface. Then every algebraic point $s \in S(\bar{k})$ lies on some rational curve, defined over $\bar{k}$.*

Proof. — Let $s \in S(\bar{k})$ be an algebraic point (on the complement to the 16 exceptional curves) and $x \in J(\bar{k})$ one of its preimages. We have proved in Corollary 2.5 that for every $x \in J(\bar{k})$ there is an endomorphism $\Phi \in \mathrm{End}_{\bar{k}}(J)$ such that $\Phi \cdot C(\bar{k})$ contains x (note that Φ commutes with the involution σ). The image of the curve $\Phi \cdot C$ in S contains s. $\square$

COROLLARY 4.3. — *Let S be a Kummer surface over a finite field k. There are infinitely many rational curves (defined over $\bar{k}$) through every point in $S(\bar{k})$ (in the complement to the 16 exceptional curves). If S is non-uniruled, these curves don't form an algebraic family.*

In addition to quotients A/σ, there exist (generalized) Kummer K3 surfaces obtained as desingularizations of abelian surfaces under actions of other finite groups. Such actions (including positive characteristic) have been classified:

PROPOSITION 4.4 (see [**10**]). — *Let A be an abelian surface over a field k and G a finite group acting on A such that the quotient A/G is birational to a K3 surface. If $\mathrm{char}(k) > 0$ then G is one of the following:*

- *a cyclic group of order* $2, 3, 4, 5, 6, 8, 10, 12$*;*
- *a binary dihedral group* $(2, 2, n)$ *with* $n = 2, 3, 4, 5, 6$*;*
- *a binary tetrahedral group* $(2, 3, 3)$*;*
- *a binary octahedral group* $(2, 3, 4)$*;*
- *a binary icosahedral group* $(2, 3, 5)$.

If $\mathrm{char}(k) = 0$ *then G is one of the following:*

- *a cyclic group of order* $2, 3, 4, 6$*;*
- *a binary dihedral group* $(2, 2, n)$ *with* $n = 2, 3$*;*
- *a binary tetrahedral group* $(2, 3, 3)$.

The groups listed above do indeed occur.

COROLLARY 4.5. — *If $S \sim A/G$ is a generalized Kummer K3 surface over a finite field k (of characteristic ≥ 7) then every algebraic point on S lies on infinitely many rational curves, defined over $\bar{k}$.*

Proof. — By Remark 3.4, a supersingular Kummer K3 surface is uniruled and the claim follows. By Lemma 6.2 in [**10**] if S is not supersingular and G is divisible by 2 then G has a unique element of order two, acting as the standard involution. An argument as in the proof of Theorem 4.2

applies to show that every algebraic point lies on a rational curve. The Kummer K3 with $G = \mathbb{Z}/5$ are supersingular.

It remains to consider $G = \mathbb{Z}/3$. In this case $A = E_0 \times E_0$ with E_0 the elliptic curve $y^2 = x^3 - 1$, with complex multiplication by $\mathbb{Z}[\sqrt{-3}]$. Let C be the genus two curve given by $y^2 = x^6 - 1$. Its Jacobian is (isogenous to) $E_0 \times E_0$. The natural $\mathbb{Z}/3$-action has eigenvalues ζ_3, ζ_3^2 and the quotient of C by this action is a rational curve. Applying the argument of Corollary 2.5 and endomorphisms (sums of powers of Frobenii, they commute with the $\mathbb{Z}/3$-action) we obtain our claim. $\square$

Remark 4.6. — There exist K3 surfaces of non-Kummer type, which are dominated by Kummer K3 surfaces. Clearly, these have the same property.

Remark 4.7. — We don't know whether or not *every* algebraic K3 surface contains infinitely many rational curves (elliptic K3 surfaces do, see [**5**]). Thus it is tempting to consider the question of lifting of rational curves on K3 surfaces from characteristic p to characteristic zero. This is analogous to deformations of rational curves on K3 surfaces over $\mathbb{C}$, where the answer is, roughly speaking, that the rational curve deforms as long as its homology class remains algebraic (see, for example, [**13**], [**5**]). If this principle applies, then every K3 surface S over $\bar{\mathbb{Q}}$ which reduces to a Kummer K3 surface modulo at least one prime, has infinitely many rational curves.

It is known that primitive classes in $\mathrm{Pic}(S)$ of a *general* K3 surface S over $\mathbb{C}$ are represented by rational curves with at worst nodal singularities (see [**24**], [**8**], for example). In particular, a general polarized S with $\mathrm{rk}\,\mathrm{Pic}(S) \geq 2$ has infinitely many rational curves. See, however, [**9**] for examples of surfaces with $\mathrm{rk}\,\mathrm{Pic}(S_{\bar{\mathbb{Q}}}) = 1$.

Remark 4.8. — Theorem 4.2 fails if $k = \mathbb{F}_q(t)$ and if S is an isotrivial Kummer surface over k. Indeed, we can think of S as a fibration over $\mathbb{P}^1$ (over $\mathbb{F}_q$) and choose a rational curve C_0 in a (smooth) fiber S_0 of this fibration. Then, for some C_0' over C_0, there is a surjective map $C_0' \times \mathbb{P}^1 \to S_0$. However, one can choose a non-uniruled (non-supersingular) S_0.

5. Surfaces of general type

Using similar ideas we can construct non-uniruled surfaces S of general type over finite fields k such that every algebraic point $s \in S(\bar{k})$ lies on a rational curve and any two points can be connected by a chain of rational curves. (However, the degrees of these curves cannot be bounded, *a priori*).

For simplicity, let us assume that $p := \mathrm{char}(k) \geq 5$. Let S_0 be a unirational surface of general type over k, for example

$$x^{p+1} + y^{p+1} + z^{p+1} + t^{p+1} = 0,$$

and $\mathbb{P}^2 \to S_0$ the corresponding (purely inseparable) covering of degree a power of p. Let S_1 be a non-supersingular (and therefore, non-uniruled) Kummer K3 surface admitting an abelian cover onto $\mathbb{P}^2$ of degree prime to p with Galois group G (for example, a double cover).

Lemma 5.1. — *For any n coprime to p, and any purely inseparable extension K/L we have a natural isomorphism*

$$K^*/(K^*)^n = L^*/(L^*)^n.$$

Proof. — Indeed, there exists an $m \in \mathbb{N}$ such L^* contains the p^m-powers of all elements of K^*. Since p^m and n are coprime the claimed isomorphism follows. $\square$

By Kummer theory, the extension of function fields $\bar{k}(S_1)$ over K is obtained by adjoining roots of elements in K^*. The extension is defined modulo $(K^*)^n$, for some n coprime to p. By Lemma 5.1, we can select a ϕ in $L^* := \bar{k}(S_0)^*$, which gives this extension. In particular, we get a diagram

$$\begin{array}{ccc} S_1 & \to & S \\ \downarrow & & \downarrow \\ \mathbb{P}^2 & \to & S_0, \end{array}$$

where S is a surface of general type (since the corresponding function field is a separable abelian extension of degree coprime to p). At the same time there is a surjective purely inseparable map $S_1 \to S$. Surjectivity implies that there is a rational curve (defined over $\bar{k}$) passing through every algebraic point of S (to get *every* point we may need to pass to a blowup $\tilde{S}_1$ of S_1 resolving the indeterminacy of the dominant map

$S_1 \to S$). Pure inseparability implies that S is non-uniruled, since S_1 is non-uniruled.

6. The case of number fields

In this section, K is a number field (with a fixed embedding into $\bar{\mathbb{Q}}$). For any nonarchimedean place v of K let k_v be the residue field at v. Let A be an absolutely simple abelian variety over K of dimension g. Assume that $\mathcal{O} := \mathrm{End}_{\bar{\mathbb{Q}}}(A)$ is an order in a field F with $[F : \mathbb{Q}] = 2\mathsf{g}$ (complex multiplication). Let S be a finite set of places of good reduction of A, A_v the corresponding abelian varieties over finite fields k_v, for $v \in \mathsf{S}$.

Lemma 6.1. — *Let C be a curve of genus $\mathsf{g}(C) \geq 2$ defined over K and $J = J_C$ its Jacobian. Assume that J is absolutely simple and has complex multiplication. Let $\{x_v\}_{v \in \mathsf{S}}$ be a set of smooth points $x_v \in J_v(k_v)$. Then there is an endomorphism $\Phi \in \mathrm{End}_{\bar{\mathbb{Q}}}(J)$ and a $c \in C(\bar{\mathbb{Q}})$ such that $\Phi(c)_v = x_v$ for any $v \in \mathsf{S}$.*

Corollary 6.2. — *In particular, let C be a hyperelliptic curve over a number field K with absolutely simple Jacobian $J = J_C$, and let σ the standard involution on J (multiplication by -1), acting as a hyperelliptic involution on $C \subset J$. Assume that J has complex multiplication. Then every point on $S \sim J/\sigma$ can be approximated by points lying on rational curves, that is, for any finite set of places S of good reduction and any set of points $s_v \in S(k_v)$ there is a point $s \in S(\bar{\mathbb{Q}})$ lying on a rational curve on S, defined over $\bar{\mathbb{Q}}$, such that s reduces to s_v, for all $v \in \mathsf{S}$.*

Proof of Lemma 6.1. — There is an $n \in \mathbb{N}$ (which we now fix) such that $x_v \in J_v[n]$, for all $v \in \mathsf{S}$. Now we choose a sufficiently large number field L/K so that $J(L) \to J_w[n]$ is a surjection for all places $w \in \mathsf{S}_L$ (the set of places of L lying over $v \in \mathsf{S}$). In particular, for all residue fields k_w, $J_w[n] \subset J_v(k_w)$ so that the corresponding Frobenii Fr_w, considered as (conjugacy classes of) elements of the Galois group $\mathrm{Gal}(\bar{L}/L)$, act trivially on $J_{w'}[n]$, for all $w' \in \mathsf{S}_L$.

Consider the map

$$\psi_w : \mathrm{End}_{\bar{\mathbb{Q}}}(J) \to \mathrm{End}_{\bar{k}_w}(J_w).$$

Since J has complex multiplication, $\psi_w(\mathrm{End}_{\bar{\mathbb{Q}}}(J))$ contains the central subfield in $\mathrm{End}_{\bar{k}}(J_w)$. Lift $\mathrm{Fr}_w \in \mathrm{Gal}(\bar{k}_w/k_w)$ to $\mathrm{End}_{\bar{k}_w}(J_w)$ and then (since it is a central element) to a global endomorphism $\Psi_w \in \mathrm{End}_{\bar{\mathbb{Q}}}(J)$.

Now we put

$$\Phi_w := \sum_{i=0}^{m-1} \Psi_w^i \in \mathrm{End}_{\bar{\mathbb{Q}}}(J),$$

with m an integer $\geq 2\mathsf{g}+1$ and congruent to $1 \mod n$) and

$$\Phi := \prod_{w \in \mathsf{S}_L} \Phi_w$$

(note that Φ_w commute in $\mathrm{End}_{\bar{\mathbb{Q}}}(J)$).

We have seen in Corollary 2.5 that for all w and all $x_w \in J_w[n]$ there exists a point $c_w \in C(\bar{k}_w)$ such that $\psi_w(\Phi_w)(c_w) = x_w$. Observe that in fact $\psi_w(\Phi)(c_w) = x_w$, for all $w \in \mathsf{S}_L$. Indeed, since $\Phi = \prod_{w' \neq w} \Phi_{w'} \cdot \Phi_w$, and $\psi_w(\Phi_{w'})$ are trivial on $x_w = \Phi_w(c_w) \in J_w[n]$ (for all $w' \in \mathsf{S}_L$), we get the claim.

To conclude, choose a point $c \in C(\bar{\mathbb{Q}})$ reducing to $c_v \in C(\bar{k}_v)$. Then $\Phi(c)$ reduces to x_v, for all $v \in \mathsf{S}$. □

7. Higher dimensions

Theorem 7.1. — *Let k be a finite field, C a hyperelliptic curve of genus ≥ 2 over k, $J = J_C$ its Jacobian abelian variety, σ the standard involution on J and $S = J/\sigma$ the associated (generalized) Kummer surface. Then every rational point $s \in S(\bar{k})$ lies on some rational curve, defined over $\bar{k}$.*

Proof. — See Theorem 4.2. □

Definition 7.2. — *A smooth projective variety V is called Calabi-Yau if its canonical class is trivial and $h^0(\Omega^i_V) = 0$ for all $i = 1, \ldots, \dim X - 1$.*

Example 7.3. — Let E an elliptic curve over k with an automorphism ρ of order 3 and $A := E^3$. The quotient A/ρ (diagonal action) admits an desingularization V with $K_V = 0$.

There are many embeddings $\iota : E \hookrightarrow A$ and, in particular, every torsion point in A lies on some $\iota(E)$.

If k is finite then every point in $V(\bar{k})$ lies on some $\bar{k}$-rational curve in V. Moreover, note that the E^2/ρ (diagonal action) is a rational surface. Hence every point in $V(\bar{k})$ lies in fact on a rational surface (defined over $\bar{k}$).

Example 7.4. — Let C be the Klein quartic curve and $J := J_C$ its Jacobian. Then the quotient of J/σ, where σ is an automorphism of order 7, admits a desingularization V which is a Calabi-Yau threefold. Again, over finite fields, one can show that every algebraic point of V lies on a rational curve.

Example 7.5. — The following varieties have been considered in [**22**]: Let S be a K3 surface with an involution σ and E an elliptic curve with the standard involution τ. Then a nonsingular model V of $E \times S/(\tau \times \sigma)$, is a Calabi-Yau threefold. If we choose S and E, defined over a finite field, so that every algebraic point of S lies on a rational curve, then the same property holds for V.

Conjecture 7.6. — Let X be any smooth projective variety over a finite field k. Assume that X has trivial canonical class and that $X_{\bar{k}}$ has trivial algebraic fundamental group. Then every algebraic point of X lies on a rational curve $C \subset X$, defined over $\bar{k}$.

Remark 7.7. — Note that if A is a general abelian variety of dimension $n \geq 3$ (over $\mathbb{C}$ or over an algebraic closure of $\bar{\mathbb{F}}_q(x)$) and σ is the standard involution, then A/σ does not contain rational curves, has trivial fundamental group and has Kodaira dimension zero (see Remark 2.1). However, the canonical class of a desingularization is nontrivial, for $n \geq 3$. This also shows that the presence of rational curves is highly unstable under deformations.

An interesting test of Conjecture 7.6 would be the case of a smooth quintic in $\mathbb{P}^4$. For some intriguing connections between the counting of points over towers of finite fields on the Calabi-Yau quintic (the Hasse-Weil zeta function) and mirror symmetry we refer to [**7**].

References

[1] A. Alzati and G. P. Pirola – "Rational orbits on three-symmetric products of abelian varieties", *Trans. Amer. Math. Soc.* **337** (1993), no. 2, p. 965–980.

[2] G. W. Anderson and R. Indik – "On primes of degree one in function fields", *Proc. Amer. Math. Soc.* **94** (1985), no. 1, p. 31–32.

[3] M. Artin – "Supersingular $K3$ surfaces", *Ann. Sci. École Norm. Sup. (4)* **7** (1974), p. 543–567 (1975).

[4] A. Beauville – "Counting rational curves on $K3$ surfaces", *Duke Math. J.* **97** (1999), no. 1, p. 99–108.

[5] F. Bogomolov and Y. Tschinkel – "Density of rational points on elliptic $K3$ surfaces", *Asian J. Math.* **4** (2000), no. 2, p. 351–368.

[6] J. Bryan and N. C. Leung – "The enumerative geometry of $K3$ surfaces and modular forms", *J. Amer. Math. Soc.* **13** (2000), no. 2, p. 371–410.

[7] P. Candelas, X. de la Ossa and F. Rodriguez-Villegas – "Calabi-Yau manifolds over finite fields, I", `hep-th/0012233`.

[8] X. Chen – "A simple proof that rational curves on $K3$ are nodal", *Math. Ann.* **324** (2002), no. 1, p. 71–104.

[9] J. Ellenberg – "K3 surfaces over number fields with geometric Picard number one", 2003, to appear.

[10] T. Katsura – "Generalized Kummer surfaces and their unirationality in characteristic p", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **34** (1987), no. 1, p. 1–41.

[11] N. M. Katz – "Space filling curves over finite fields", *Math. Res. Lett.* **6** (1999), no. 5-6, p. 613–624.

[12] ———, *Twisted L-functions and monodromy*, Annals of Mathematics Studies, vol. 150, Princeton University Press, Princeton, NJ, 2002.

[13] S. Mori and S. Mukai – "The uniruledness of the moduli space of curves of genus 11", Algebraic geometry (Tokyo/Kyoto, 1982), Lecture Notes in Math., vol. 1016, Springer, Berlin, 1983, p. 334–353.

[14] D. Mumford – *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[15] F. Oort and J. de Jong – "Hyperelliptic curves in abelian varieties", *J. Math. Sci.* **82** (1996), no. 1, p. 3211–3219, Algebraic geometry, 5.

[16] G. P. Pirola – "Curves on generic Kummer varieties", *Duke Math. J.* **59** (1989), no. 3, p. 701–708.

[17] B. Poonen – "Néron-Tate projection of algebraic points", *Internat. Math. Res. Notices* (2001), no. 9, p. 435–440.

[18] F. Pop and M. Saidi – "On the specialization homomorphism of fundamental groups of curves in positive characteristic", Galois groups and fundamental groups (L. Schneps, ed.), MSRI Publications, vol. 41, Cambridge Univ. Press, 2003, p. 107–118.

[19] A. N. Rudakov and I. R. Shafarevich – "Supersingular $K3$ surfaces over fields of characteristic 2", *Izv. Akad. Nauk SSSR Ser. Mat.* **42** (1978), no. 4, p. 848–869.

[20] ______, "Surfaces of type $K3$ over fields of finite characteristic", Current problems in mathematics, Vol. 18, Akad. Nauk SSSR, 1981, p. 115–207.

[21] T. Shioda – "Some results on unirationality of algebraic surfaces", *Math. Ann.* **230** (1977), no. 2, p. 153–168.

[22] C. Voisin – "Miroirs et involutions sur les surfaces $K3$", *Astérisque* (1993), no. 218, p. 273–323, Journées de Géométrie Algébrique d'Orsay (Orsay, 1992).

[23] A. Weil – "Zum Beweis des Torellischen Satzes", *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.* **1957** (1957), p. 33–53.

[24] S.-T. Yau and E. Zaslow – "BPS states, string duality, and nodal curves on $K3$", *Nuclear Phys. B* **471** (1996), no. 3, p. 503–512.